Betrieb sicherer Netzinfrastrukturen für Grid-Umgebungen

Christian Grimm, Jan Wiebelitz, Stefan Piger, Denis Göhr

Regionales Rechenzentrum für Niedersachsen (RRZN)
Universität Hannover
Schloßwender Straße 5, 30159 Hannover
{grimm,wiebelitz,piger,goehr}@rrzn.uni-hannover.de

Zusammenfassung: Die typisch in Grid-Umgebungen eingesetzte Middleware Globus Toolkit 2.4 und 4.0 sowie LCG2 und gLite liefern zunehmend komplexe Verfahren für Authentifizierung und Autorisierung von Nutzern, Daten, Services und Ressourcen. Auch wenn konkrete Implementierungen zum Teil noch nicht vorliegen, sind vielversprechende Konzepte erkennbar. Demgegenüber stellt der Einsatz von Firewalls aufgrund der komplexen Kommunikationsbeziehungen und Anwendungsprotokolle in Grids ein weitgehend ungelöstes Problem dar. Als einzige Lösung werden typisch weite Bereiche auf den Firewalls freigeschaltet oder Firewalls vollständig überbrückt, was einem verantwortungsvollen Schutz von Ressourcen in Grids widerspricht. Mittelfristige Lösungen zur Minderung dieses Problems sind jedoch nicht in Sicht.

1 Einleitung

Der Aufbau sicherer Netzinfrastrukturen für Grid-Umgebungen ist ein bisher weitgehend ungelöstes Problem. Die Anforderung, zum Teil mobile Teilnehmer zu den Ressourcen Virtueller Organisation zuzulassen, stellt sowohl Entwickler als auch Betreiber solcher Umgebungen vor bisher unbekannte Herausforderungen. Die zuverlässige Authentisierung der Nutzer ist zwar durch den Einsatz von PKIs und so genannten Proxy-Zertifikaten in Grids fest etabliert, umfassende Verfahren zur Autorisierung sind jedoch gegenwärtig nur in Ansätzen implementiert.

Neben der Kontrolle des Zugangs sowie der autorisierten Nutzung von Ressourcen ist die Absicherung der Netze ein weiterer wichtiger Aspekt sicherer Netzinfrastrukturen. Aufgrund der hohen Anforderungen bezüglich Durchsatz und Variabilität der Protokolle wurden Firewalls bisher kaum in Grid-Umgebungen eingebunden [NaRi04]. Hierdurch liegen jedoch die Ressourcen in Grids einschließlich der zum Teil hochsensitiven gespeicherten Daten potentiellen Angreifern offen. Diese Situation ist besonders kritisch, da die in Grids eingesetzte Middleware durch intensive Nutzung netzbasierter Kommunikationsabläufe eine Vielzahl potentieller Angriffspunkte bietet und bisher kaum hinsichtlich Sicherheitsanforderungen implementiert oder sogar durch Code Reviews geprüft wurde.

Mit unserem Beitrag liefern wir einen Überblick über den aktuellen Stand der Absicherung von Grid-Umgebungen, insbesondere über Infrastrukturen zur Authentifizierung und Autorisierung (AAI) sowie über Firewalls, und geben einen Ausblick auf zukünftige Entwicklungen in diesen Bereichen. Dabei gehen wir besonders auf die Situation aus Sicht

von Hochschulrechenzentren ein, die als Betreiber von Netzinfrastrukturen häufig bisher nur mittelbar in den Aufbau von Grid-Umgebungen involviert waren. Die eigentlichen Nutzer mit ihren Grid-Anwendungen sowie die Anbieter der Grid-Ressourcen stammen als treibende Kraft für den Einsatz dieser Technologie typisch aus Instituten oder Forschungseinrichtungen innerhalb der Hochschule. Durch zukünftig steigende Anforderungen an die Sicherheit solcher Umgebungen werden jedoch auch die Rechenzentren zunehmend mit Grid-spezifischen Fragestellungen konfrontiert.

2 Betrachtete Grid Middleware

2.1 Globus Toolkit

Das Globus Toolkit stellt die erste Middleware dar, die mit einer eindeutigen Ausrichtung auf das Grid-Computing entwickelt wurde Unter Federführung der drei Institutionen Argonne National Laboratory, University of Southern California und University of Chicago wurde 1998 die Version 1 des Globus Toolkit freigegeben.

Wurde das Globus Toolkit ursprünglich für Anwendungen aus der Hochenergiephysik (HEP) entwickelt, wird es mittlerweile in zahlreichen Forschungsprojekten, u. a. aus den Bereichen Astrophysik, Klima- und Wetterforschung oder Bioinformatik eingesetzt. Das Globus Toolkit stellt somit heute einen de facto Standard für Grid Middleware dar.

In Produktivumgebungen wird zurzeit Version 2 des Globus Toolkit eingesetzt. Es besteht aus den grundlegenden Komponenten für

- Ressource Management,
- Data Management,
- Information Service.

Sämtliche Komponenten basieren auf der *Grid Security Infrastructure* (GSI), die ebenfalls Bestandteil des Globus Toolkit ist. Eine ausführliche Beschreibung von GSI erfolgt in Abschnitt 3.2.1.

Das Globus Toolkit bietet jedoch noch kein vollständiges Framework für Grid Computing, so dass für den Betrieb weitere Komponenten notwendig sind. So muss z. B. über vorhandene Schnittstellen ein Batchsystem wie Condor oder PBS eingebunden werden. Als Beispiele für weitere Komponenten lassen sich Portale für den Zugang zu Grids, Services zur Realisierung erhöhter Sicherheitsanforderungen oder Verfahren für Accounting und Billing anführen, die in zahlreichen, typisch internationalen Projekten entwickelt werden.

Eine wesentliche Änderung erfolgte Ende April 2005 mit der Freigabe des Globus Toolkit in der Version 4.0. Zur Vereinheitlichung der Kommunikation werden zwischen den Komponenten ab dem Globus Toolkit 4.0 weitgehend Web Services gesetzt. Ein Überblick über die zum Teil noch in der Konzeption befindlichen Sicherheitsmerkmale von Web Services erfolgt in Abschnitt 3.3.1.

2.2 LCG und gLite

In 2007 wird der Produktionsbetrieb des *Large Hadron Collider* (LHC) am CERN gestartet. Der LHC besteht aus den vier Experimenten der Hochenergiephysik ALICE, ATLAS,

CMS und LHCb, für die jeweils eigene Detektoren um den Beschleunigerring aufgebaut werden. Im Rahmen der Bemühungen, eine geeignete Infrastruktur zur Verarbeitung der anfallenden Datenmengen von bis zu 15 Petabyte pro Jahr aufzubauen, entsteht das *Large Hadron Collider Computing Grid* (LCG). Dabei sollen die Daten in einer vierstufigen Hierarchie global verteilt werden. Die einzelnen Partner innerhalb einer Hierarchiestufe werden die Detektordaten von Einrichtungen der jeweils nächst höheren Ebene zur Verfügung gestellt bekommen und verarbeiten. Die Planungen sehen vor, eine Prozessorleistung von ca. 100.000 CPUs auf dem Niveau von 2004 bei Inbetriebnahme des LHCs zur Verfügung stellen zu können.

Um die Rechenleistung und Speicherkapazität effizient einzusetzen, wird eine eigene Grid Middleware mit dem Namen LCG2 auf Basis des Globus Toolkits entwickelt. LCG2 ist momentan in der Release 2.4 verfügbar und wird produktiv vor allem in der HEP-Community eingesetzt.

Parallel zu den Arbeiten an LCG wurde das von der EU geförderte Projekt *Enabling Grids for E-sciencE* (EGEE) im April 2004 gestartet. Es läuft über einen Zeitraum von zwei Jahren und hat zum Ziel, mindestens 3.000 Nutzern eine Grid-Umgebung von 8.000 CPUs produktiv zur Verfügung zu stellen. EGEE verwendete als Middleware bei Projektstart LCG2. Diese wurde sukzessiv weiterentwickelt und durch weitere Komponenten ergänzt. Das daraus entstandene Paket wurde mittlerweile in gLite umbenannt. Im April 2005 erschien die erste Version 1.0 von gLite, die ab Juli 2005 von den vier LHC-Experimenten eingesetzt werden soll.

EGEE plant, neben HEP auch weitere Communities in die Nutzung und Weiterentwicklung von gLite einzubinden. Bereits in 2005 sollen insbesondere Nutzergruppen aus der Bioinformatik, Astronomie, sowie Geophysik und Chemie gewonnen werden.

3 Sicherheitsarchitekturen für Grid Middleware

3.1 Public Key Infrastructure

Die Mehrzahl der heute verwendeten Grid Middleware setzt für die Authentifizierung sowohl der Services als auch der Nutzer eine *Public Key Infrastructure* (PKI) voraus. Eine PKI ermöglicht die vertrauensvolle Kommunikation zwischen unbekannten Partnern über eine vertrauenswürdige Instanz, die *Certificate Authority* (CA). Wesentliches Element einer PKI ist die asymmetrische Verschlüsselung. Hierbei wird ein Paar von zwei verschiedenen Schlüsseln benötigt, um Daten ver- und entschlüsseln zu können. Der so genannte Public Key wird veröffentlicht und muss sämtlichen Kommunikationspartner zur Verfügung stehen, während der Private Key nur für den eigenen Zugriff bestimmt ist und vor Dritten verborgen gehalten werden muss [MOV96].

Durch die Signatur der CA wird in X.509 Zertifikaten die Zusammengehörigkeit von Public Key und einem *Distinguished Name* (DN) beglaubigt. Der Distinguished Name ist der eindeutige Name des Schlüsselinhabers und beinhaltet neben dem Namen auch Angaben über dessen Zugehörigkeit zu einer Organisation:

```
CN = Erika Mustermann, OU = UniHannover, O = GermanGrid, C = DE
```

Der Schlüsselinhaber ist eine natürliche Person oder auch ein System.

Um Zertifikate vor dem eigentlichen Ablauf ihres Gültigkeitsdatums für ungültig zu erklären, werden sie zurückgerufen. Für den Rückruf von Zertifikaten gibt es derzeit zwei Ansätze. Das erste Verfahren umfasst das Erstellen einer Liste von ungültigen oder kompromittierten Zertifikaten durch die CA. Diese *Certificate Revocation List* (CRL) wird durch die CA signiert und veröffentlicht. CRLs müssen in regelmäßigen Abständen erneuert und von allen Systemen, die Zertifikate einer CA akzeptieren, bezogen werden. Dies erfolgt in der Regel mittels HTTP(S).

Der zweite und neuere Ansatz wird vom *Online Certificate Status Protocol* (OCSP) verfolgt, um bereits während der Authentifizierungsphase online die Gültigkeit eines Zertifikates abfragen zu können. Der Vorteil dieses Verfahrens liegt in einer verbesserten Aktualität durch die direkte Abfrage des Zertifikatsstatus bei der Zertifizierungsautorität, da die Aktualisierung von CRLs in der Regel nur in mehrstündigen Intervallen erfolgt.

3.1.1 PKIs für Grid Computing in Deutschland

Ein Ergebnis des fünften Rahmenprogramms der Europäischen Union ist eine beispielhafte Policy für Zertifizierungsstellen, die von der *European Policy Management Authority for Grid Authentication in e-Science* (EUGridPMA) erstellt wird.

In Deutschland sind zurzeit zwei Zertifizierungsstellen in Betrieb, die Zertifikate für Grid Communities nach der EUGridPMA-konformen Policy ausstellen. Am Forschungszentrum Karlsruhe ist die deutsche CA für das LCG angesiedelt und vorrangig für Teilnehmer aus der HEP-Community zuständig. Der DFN-Verein betreibt eine eigene CA für Teilnehmer weiterer Communities.

Um Nutzern die Beantragung von Zertifikaten dieser beiden CAs zu erleichtern, ist der Aufbau regionaler *Registration Authorities* (RA) sinnvoll. Diese RAs signieren den Zertifizierungsantrag lokaler Antragsteller nach Prüfung von deren Identität und leiten den Antrag an die CA weiter. Aufgrund der Vertrauensstellung der RAs zu der jeweiligen CA brauchen die Nutzer nicht bei der CA vorstellig zu werden. Die ausgestellten Zertifikate werden den Nutzern per E-Mail zugestellt.

3.2 Globus Toolkit 2.4

3.2.1 Grid Security Infrastructure

Basierend auf SSL/TLS, PKIs und X.509 Zertifikaten bietet die *Grid Security Infrastructure* (GSI) eine einheitliche Schnittstelle, um erweiterte Sicherheitsfunktionen in den Komponenten des Globus Toolkit zu nutzen. Bestehende freie Software wie OpenSSH[1] oder WU-FTPD[2] wurde mit Hilfe des GSI für das Grid Computing im Globus Toolkit adaptiert.

Im Wesentlichen liefert GSI folgende allgemeine Funktionen:

[1] http://www.openssh.org/

[2] http://www.wu-ftpd.org/

- ein- und gegenseitige Authentifizierung,
- vertrauliche Kommunikation,
- Autorisierung,
- Single Sign-On,
- Delegation.

Eine Authentifizierung findet stets zwischen zwei Instanzen statt und kann in der GSI sowohl einseitig als auch gegenseitig erfolgen. Bei einseitiger Authentifizierung sendet z. B. ein Nutzer sein X.509 Zertifikat, d. h. seinen signierten Public Key, an eine Ressource. Die Ressource validiert zunächst das Zertifikat durch Prüfung der Gültigkeit, der ordnungsmäßigen Signatur durch die CA und anhand der CRL der CA. Anschließend antwortet sie mit einer unverschlüsselten zufälligen Zahlenfolge. Der Nutzer verschlüsselt die Zahlenfolge mit seinem Private Key und sendet das Ergebnis an die Ressource. Die Ressource kann diese Daten wieder mit dem Public Key aus dem X.509 Zertifikat des Nutzers entschlüsseln. Bei positivem Vergleich mit der ursprünglich generierten Zahlenfolge ist der Nutzer erfolgreich und zuverlässig authentifiziert (siehe Abbildung 1) [FBA+03]. Bei gegenseitiger Authentifizierung wird der Prozess der einseitigen Authentifizierung von beiden Instanzen wechselseitig durchgeführt.

Nach der Authentifizierung ist die Autorisierung die zweite Komponente, die es erlaubt, den Zugriff auf Systeme kontrolliert zu beschränken. Nach einer erfolgreichen Authentifizierung durch ein X.509 Zertifikat wird der Distinguished Name des Zertifikats durch das so genannte *grid-mapfile* auf einen lokalen UNIX-Account abgebildet (siehe Abbildung 1). Die lokalen Prozesse auf der Ressource werden mit den Rechten dieses Accounts ausgeführt.

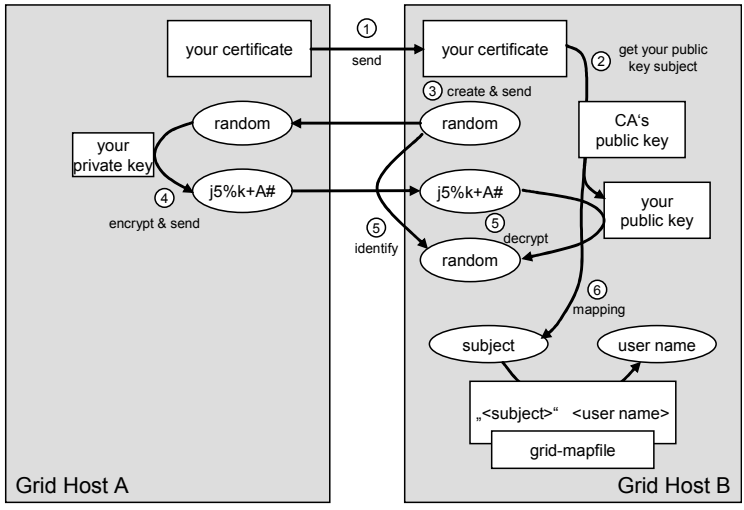

Abbildung 1: Authentifizierung und Autorisierung im Globus Toolkit 2.4

Eine mit GSI eingeführte, für Grid-Umgebungen unumgängliche Erweiterung bestehender Sicherheitsinfrastrukturen stellen die so genannten Proxy-Zertifikate dar, die zur Delegierung von Berechtigungen und zur Authentifizierung genutzt werden. Proxy-Zertifikate sind mit dem Private Key des Nutzers signiert (siehe Abbildung 2) und haben eine verhältnismäßig kurze Gültigkeitsdauer. Die Gültigkeitsdauer eines Proxy-Zertifikats wird allgemein in den Policies der zugehörigen Virtuellen Organisation geregelt und kann wenige Minuten bis mehrere Stunden betragen.

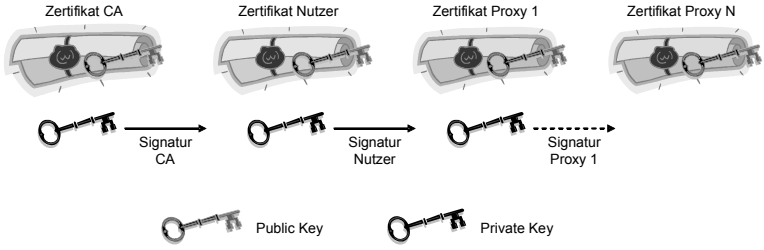

Abbildung 2: Zertifikatskette mit Proxy-Zertifikaten

Mit dem Private Key eines Proxy-Zertifikates können wiederum neue Proxy-Zertifikate signiert werden. Proxy-Zertifikate können somit von Kindprozessen der abgegebenen Jobs zur Authentifizierung genutzt werden (siehe Abbildung 3). Durch die Zertifikatskette, die sich durch ein oder mehrere Proxy-Zertifikate, das Nutzer-Zertifikat und das Zertifikat einer CA bildet, sind Proxy-Zertifikate vertrauenswürdig.

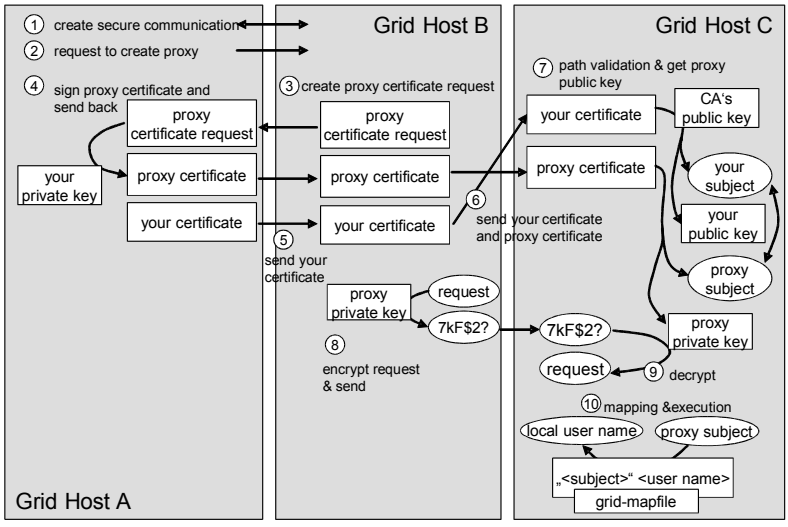

Abbildung 3: Delegation durch Proxy-Zertifikate

Durch die Nutzung von Proxy-Zertifikaten ist eine einmalige Authentifizierung des Nutzers ausreichend, da Prozesse sich bei Bedarf eigene Proxy-Zertifikate zur Authentifizierung erzeugen können. Der Nutzer delegiert somit seine Berechtigung für die Gültigkeitsdauer des Proxy-Zertifikates an den Prozess, der dieses Proxy-Zertifikat nutzt. Hierdurch wird eine wesentliche Forderung für das Grid Computing, das Single Sign-On gegenüber einer Grid-Infrastruktur, gewährleistet.

3.2.2 Virtuelle Organisationen

In [FKT01] wurde das Konzept der *Virtuellen Organisation* (VO) eingeführt. Eine VO ist ein dynamischer Zusammenschluss von Entitäten (Nutzer und Systeme), die ein gemeinsames Projekt bearbeiten. Sie bieten die Möglichkeit, grenzübergreifend zwischen verschiedenen Ländern, Firmen oder Institutionen zusammenzuarbeiten. Authentifizierung und Autorisierung innerhalb einer VO erfolgt durch X.509 Zertifikate und Proxy-Zertifikate. Für eine VO existiert mindestens eine CA, die X.509 Zertifikate für die beteiligten Instanzen herausgibt.

3.3 Globus Toolkit 4.0

Das Globus Toolkit 4.0 ist eine direkte Weiterentwicklung des Globus Toolkit 2.4. Die in Abschnitt 3.2 aufgeführten Sicherheitsmerkmale sind daher weitgehend auch im Globus Toolkit 4.0 enthalten.

3.3.1 Web Services

Eine wesentliche Neuerung im Globus Toolkit 4.0 ist die Einführung von *Web Services* (WS) für die Kommunikation zwischen den Grid-Komponenten. Durch Web Services wird die Kommunikation der Grid-Komponenten über standardisierte Schnittstellen (SOAP über HTTP und HTTPS) geführt.

WS-Security bietet eine gesicherte und geschützte Übertragung von SOAP-Messages. Basierend auf WS-Security veröffentlichten u. a. IBM, Microsoft, SAP und VeriSign sechs weitere Spezifikationen, um den Aufbau vertrauensvoller Beziehungen, den geschützten Austausch von Nachrichten und verschiedene Stufen der gesicherten Übertragung zwischen Grid-Komponenten zu gewährleisten (siehe Abbildung 4).

Folgende sechs Spezifikationen basieren auf WS-Security [DDF+02]:

1. WS-Policy bietet einen Standard, um die Möglichkeiten und Begrenzungen einer Security Policy (z. B. verwendete Security Tokens oder Verschlüsselungsalgorithmen) zu beschreiben. Um die Policies in XML geeignet zu beschreiben, wird die *eXtensible Access Control Markup Language* (XACML) genutzt.
2. WS-Trust beschreibt ein Modell das es erlaubt, zwischen Web Services eine vertrauensvolle/verlässliche Beziehung (trust relationship) aufzubauen. Diese vertrauensvolle Beziehung ist für die Ausgabe von XML-Signaturen, PKI und das XML Key Management notwendig.

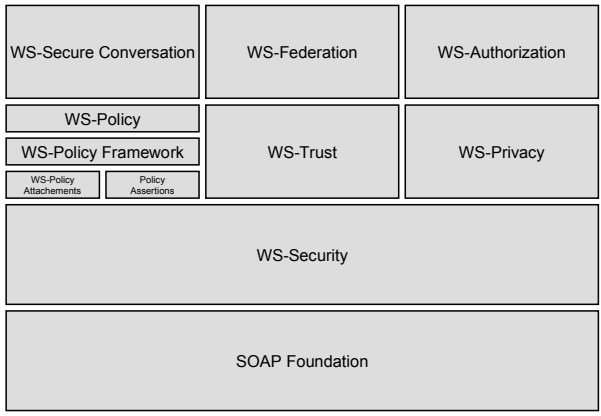

Abbildung 4: WS-Security als Basis für weitere Spezifikationen

3. WS-Privacy bietet ein Modell zum Schutz der Privatsphäre einzelner und zur Durchsetzung vom Privacy Practice Statements von Unternehmen.
4. WS-Secure Conversation spezifiziert die Methoden für einen authentifizierten Nachrichtenaustausch zwischen WS-Komponenten. Die Spezifikation enthält Aussagen über den Austausch eines Sicherheitskontextes und der benötigten Session Keys.
5. WS-Federation spezifiziert den Aufbau einer vertrauensvollen Beziehung in einem heterogenen Verbund verschiedener Institutionen.
6. WS-Authorization regelt den Transport von Berechtigungsattributen.

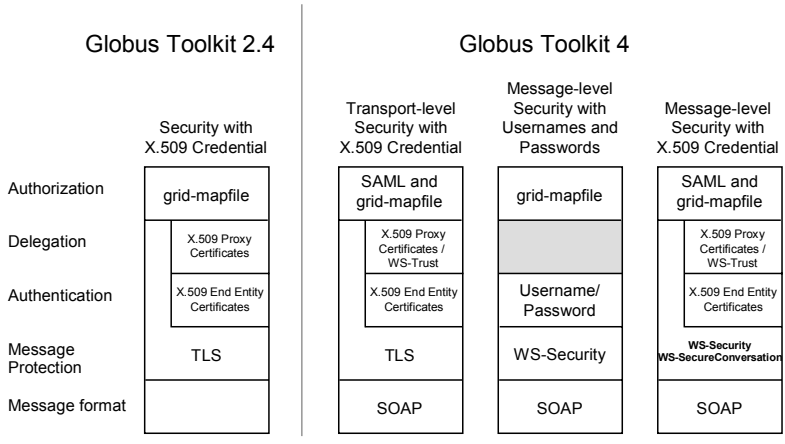

Abbildung 5: Sicherheitsarchitekturen von Globus Toolkit 2.4 und 4.0

Abbildung 5 stellt zusammenfassend die Sicherheitsarchitekturen von Globus Toolkit 2.4 und 4.0 gegenüber [Wel04]. Zu beachten ist, dass in Globus Toolkit 4.0 auch die Architek-

tur der Version 2.4 enthalten ist. Neben der Rückwärtskompatibilität ist die derzeit mangelnde Performance von Web-Services ein wesentlicher Grund für diesen Ansatz.

3.3.2 MyProxy

Ein für die Sicherheit von Grid-Umgebungen wichtiger Aspekt ist die sichere Verwahrung von Authentifizierungsdaten (Credentials) der Nutzer. Die Speicherung dieser Daten auf der Festplatte des eigenen PCs bietet keinen geeigneten Schutz und ist deshalb untauglich. Alternativ bietet sich der Einsatz externer Speichermedien wie Hardware Tokens oder Smart Cards an. Einen weiterführenden Ansatz stellen jedoch netzbasierte Services zur zentralen Speicherung der Credentials dar. Derartiges Systeme werden als Credential Repository, aber auch als Virtual Smart Card oder Credential Wallet bezeichnet.

Credential Repositories sind typisch gehärtete Systeme, auf denen ausschließlich der Dienst zur Verwaltung von Authentifizierungsdaten zur Verfügung steht. Das Globus Toolkit 4.0 beinhaltet das Online Credential Repository MyProxy[3]. MyProxy speichert X.509 Proxy-Zertifikate und die zugehörigen Private Keys, geschützt durch Passphrase, Zertifikat, Kerberos, PAM und One-Time-Passwords. MyProxy kann für die Authentifizierung an Grid-Portalen und für die Erneuerung von Proxy-Zertifikaten (Proxy-Credentials) genutzt werden. Neben dem Schutz von Authentifizierungsdaten kann MyProxy auch die Erstellung von Proxy-Zertifikaten und deren automatische Verlängerung für langlaufende Jobs durchführen.

3.3.3 Community Authozation Service

Der *Community Authorization Service* (CAS) wurde im Globus Toolkit 3 eingeführt und wird zurzeit auch im Globus Toolkit 4.0 durch GridFTP genutzt. CAS erlaubt es, Anbietern von Ressourcen *Access Control Policies* (ACP) für gesamte Communities zu formulieren, während die Berechtigungen feinerer Granularität innerhalb der Communities gepflegt werden. Hierdurch behalten die Anbieter die übergeordnete Kontrolle über ihre Ressourcen, während Tätigkeiten wie die Pflege der Nutzer-Accounts den Communities übertragen werden.

Vor dem Zugriff auf eine Ressource beantragt der Nutzer beim CAS-Server ein Proxy-Zertifikat. Der CAS-Server integriert in das beantragte Proxy-Zertifikat Informationen über die Berechtigungen des Nutzers. Mit dem Proxy-Zertifikat authentifiziert sich somit der Nutzer an der Ressource und übergibt dabei gleichzeitig Informationen über seine Berechtigungen.

3.3.4 LCG und gLite

LCG bzw. gLite basieren auf Komponenten des Globus Toolkit und enthalten somit ebenfalls die grundlegenden Sicherheitsmechanismen der GSI. Da LCG und gLite jedoch den

[3] http://grid.ncsa.uiuc.edu/myproxy/

weiterführenden Ansatz einer vollständigen Grid-Umgebung verfolgen, wird die derzeitige Sicherheitsarchitektur von gLite gegenüber dem Globus Toolkit um weitere Komponenten bzw. Funktionalität ergänzt (Abbildung 6).

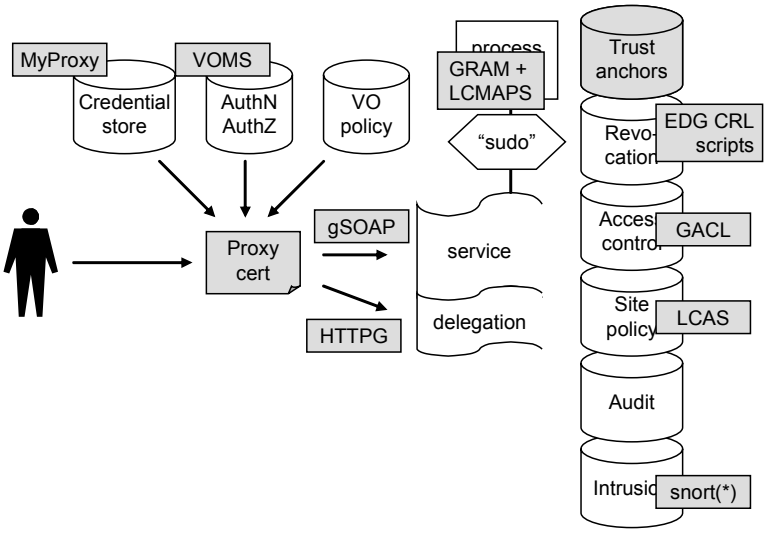

Abbildung 6: Sicherheitsarchitektur gLite

3.3.5 Authentifizierung

Der Nutzer präsentiert bei der Authentifizierung in gLite-Umgebungen dem zu nutzenden Dienst seine relevanten Credentials, insbesondere sein (Proxy-)Zertifikat (s. Abbildung 6), d. h. es wird nach dem Push-Modell gearbeitet. Derzeit wird in gLite auch eine Authentifizierung nach dem Pull-Modell untersucht. Dieses Modell ist insbesondere in Fällen sinnvoll, in denen Institutionen einer bestehenden Gruppe von Nutzern (z. B. Studenten) Zugriff auf Grid-Ressourcen ermöglichen wollen. Dies kann z. B. über einen föderativen Ansatz erfolgen, den man bei Shibboleth[4] findet.

Um die fälschliche Akzeptierung von zurückgerufenen Zertifikaten zu verhindern, setzt gLite auf das*Online Certificate Status Protocol*. Es werden jedoch auch CRL-basierte Validitätsüberprüfungen von Zertifikaten unterstützt, um als Backup im Falle einer Netzwerkpartitionierung verwendet werden zu können. Die Unterstützung von OCSP ist in der Release 1.0 von gLite allerdings noch nicht enthalten, so dass im Augenblick ausschließlich CRLs Verwendung finden.

gLite verwendet, wie das Globus Toolkit 4.0, das Online Credential Repository MyProxy für die Speicherung und Verbreitung von Credentials.

[4] http://shibboleth.internet2.edu

3.3.6 Autorisierung

gLite unterscheidet zwischen globaler und lokaler Autorisierung. Die globale Autorisierung findet auf Ebene der Virtuellen Organisation statt, während die lokale Autorisierung von der Ressource vorgenommen wird. Die globale Autorisierung und Unterstützung von Virtuellen Organisationen wird in gLite über den *Virtual Organisation Membership Service* (VOMS, Abbildung 6) realisiert. VOMS ordnet Nutzern eine VO und eine Rolle innerhalb dieser VO zu. Rechte werden aus diesen beiden Attributen abgeleitet. Die Attribute werden in das vom VOMS-Server erstellte Proxy-Zertifikat eingebettet, so dass die Nutzer bei der Authentifizierung an der gewünschten Ressource ihre Rechte nachweisen können. Lokale Entscheidungen zur Autorisierung, die in der Ressource getroffen werden, sind über das gridmap-file realisiert.

Das Autorisierungsmodell von gLite basiert momentan auf dem Push-Ansatz, es sind jedoch Weiterentwicklungen insbesondere in Richtung Agent-Modell vorgesehen. Für spätere Releases sind Autorisierungsmechanismen geplant, die auf der *Security Assertion Markup Language* (SAML) und XACML basieren.

3.4 Firewalls

Firewalls sind heute sowohl für den Aufbau als auch den Betrieb sicherer Netzinfrastrukturen und klassischer Netzdienste anerkannt unverzichtbar. Auch die in Grids gespeicherten und bearbeiteten Daten, der Zugang zu den VOs sowie der Betrieb der für Grids integralen Netzdienste, wie z. B. einer PKI oder Directory- und Accounting-Services, sind sowohl vor unbefugten Zugriffen als auch vor kompromittierenden Angriffen zu schützen. Die Anwendungen in einer Grid-Umgebung und die daraus resultierenden Anforderungen an Firewalls unterscheiden sich jedoch erheblich von gewöhnlichen Campus-Netzen oder Server-Umgebungen. Zum einen stellen die Anwendungen extreme Durchsatz- und Latenz-Anforderungen [DAH+04], zum anderen kommen spezielle Grid-Protokolle zum Einsatz, die von Firewalls nicht interpretiert werden können und für die daher kein aktiver Schutz geboten werden kann. Für diese Probleme gibt es heute keine akzeptablen Lösungen. Aktuelle prototypische Grids nutzen Umgehungen von Firewalls, die sich weder vom administrativen Aufwand noch vom gebotenen Sicherheitsstandard auf einen Regelbetrieb übertragen lassen.

Für die Datenübertragung zwischen verschiedenen Systemen wurde im Globus Toolkit 2 mit GridFTP ein leistungsfähiges, sicheres und robustes Protokoll entwickelt. GridFTP basiert auf dem FTP-Protokoll und fügt diesem für Grid-Umgebungen notwendige Erweiterungen hinzu:

- Vollständige Integration der GSI, d. h. bei Bedarf gegenseitige Authentifizierung mittels Zertifikaten und komplette Verschlüsselung des Datenstroms.
- Dateitransfer von definierten Segmenten, um nicht die vollständige Datei von zum Teil mehreren Gigabyte übertragen zu müssen.
- Paralleler Datentransfer über mehrere TCP-Datenströme zur Erhöhung des gesamten Durchsatzes oder zum gleichzeitigen Lesen bzw. Schreiben auf Speicherelemente im Grid.

- Third-Party Datentransfers (s. Abbildung 7) ermöglichen, von einem entfernten GridFTP-Clienten die direkte Datenübertragung zwischen zwei GridFTP-Servern zu steuern.

Besonders die beiden letztgenannten Punkte bereiten bei der Integration von Firewalls in Grid-Umgebungen erhebliche Probleme. Aus ein- und ausgehenden parallelen Datentransfers resultiert in der Regel eine hohe Anzahl von TCP-Verbindungen, für die große Portbereiche in den Firewalls – auch für eingehende Verbindungen – permanent geöffnet werden müssen.

Vergleichbare Probleme mit herkömmlichen Anwendungsprotokollen wie FTP werden in Firewalls typisch durch die Funktion eines Application Level Gateways gelöst. Hierbei enthält die Firewall einen vollständigen Parser zur Analyse und Interpretation des FTP-Protokolls. Die Firewall ist somit in der Lage, die Parameter, die Client und Server für den Aufbau des Datenkanals aushandeln, aus dem Kontrollkanal auszulesen und automatisch entsprechende Ressourcen temporär freizugeben. Aufgrund des derzeit geringen kommerziellen Interesses werden entsprechende Application Level Gateways für Grid-Protokolle in Firewalls auch mittelfristig kaum zur Verfügung stehen.

Ein weiteres Problem bei dem Einsatz von Firewalls in Grid-Umgebungen stellt die Möglichkeit dar, einen Datentransfer zwischen zwei GridFTP-Servern von einer dritten Instanz zu initiieren (siehe Abbildung 7). Bei dieser Form des so genannten Third-Party Datentransfers baut der Client jeweils eine Kontrollverbindung zu jedem der beiden Server auf. Zwischen den Servern bestehen nur die Verbindungen für den eigentlichen Transfer der Nutzdaten. Da die Initiierung von keinem der an der eigentlichen Datenübertragung beteiligten Server ausgeht, haben Firewalls zwischen den GridFTP-Servern keine Möglichkeit, die Legitimität der Verbindungen zu prüfen.

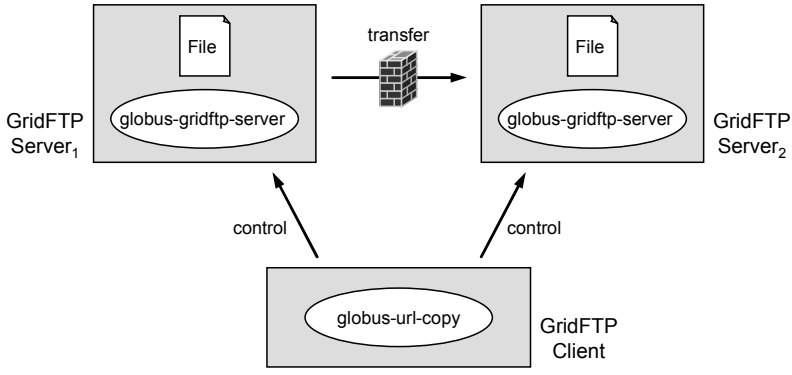

Abbildung 7: Datentransfer zwischen GridFTP-Servern

Da die Transferverbindungen verschlüsselt sein können, wären auch hieraus keine Hinweise zu gewinnen, ob diese Verbindungen tatsächlich berechtigt sind. Dies gilt auch unter der Annahme, dass Firewalls das GridFTP-Protokoll beherrschen. Eine Authentifizierung je-

der Transferverbindung mit Hilfe der jeweiligen Server-Zertifikate ist dabei möglich und muss auch verbindlich sein, um einen Missbrauch der offenen Ports auf der Firewall für Angriffe zu minimieren.

Die Sicherheit der Netze mit GridFTP-Servern beruht folglich zu einem sehr hohen Teil auf der Sicherheit der Server selbst, da sie durch die Firewall nicht zuverlässig geschützt werden können. Bei Kompromittierung der Server ist damit auch das Netz, in dem sich die Server befinden, kompromittiert. Daher sollten alle an einem Grid beteiligten Geräte in einer separaten *Demilitarisierten Zone* (DMZ) platziert werden, um die Auswirkung einer Kompromittierung möglichst gering zu halten. Eine hohe Sicherheit aller in dieser DMZ befindlichen Rechner ist dabei unerlässlich.

3.5 Entwicklungen

Als Ausweg aus dieser nicht zufrieden stellenden Situation wird derzeit die dynamische Konfiguration von Firewalls diskutiert, d. h. die automatisierte Aktivierung transienter Regeln. Für die Integration in bestehende Middleware existieren prinzipiell zwei mögliche Ansätze, wobei die Kommunikation häufig nicht direkt mit den Firewalls, sondern über Proxies (so genannte Opener) abläuft. Zum einen kann der Firewall direkt ein Verbindungswunsch authentifiziert und autorisiert mitgeteilt werden. Eine Implementierung dieser so genannten In-Band-Signalisierung ist die bereits in Grids eingesetzte Dyna-Fire [GGM04]. Hierbei wird das so genannten *Port Knocking* verwendet, bei dem vorgegebene Vektoren von Ports adressiert werden müssen, um Regeln auf den Firewalls zu aktivieren. Ein alternatives Verfahren wird in [Hil02] durch Senden eines so genannten Globus *ping* beschrieben. Der zweite Ansatz verfolgt eine Out-of-Band-Signalisierung, wie sie aus dem Bereich der Intrusion Prevention Systeme bekannt ist. Als Beispiel hierfür kann das Open Platform for Security (OPSEC) Framework[5] für kommerzielle Firewalls genannt werden.

4 Ausblick

Außerhalb der eigentlichen Entwicklungen des Globus Toolkit oder gLite werden in weiteren Projekten Ansätze zur Verbesserung der Sicherheitsarchitekturen in Grids erarbeitet. So sorgt z. B. das Projekt GridShib[6] für neue Verfahren der Autorisierung im Globus Toolkit 4.0. In anderen Projekten werden formale Methoden zur Formulierung von Policies und Service Level Agreements, aber auch von Rechten zur Authentifizierung und Autorisierung untersucht. Insgesamt sind für den Bereich der Autorisierung, der bisher durch den rudimentären Ansatz des grid-mapfile gegenüber der Authentifizierung nicht ausgereift erscheint, zukünftig umfassende Verbesserungen zu erwarten.

Weitere Entwicklungen werden auch durch die Erschließung neuer Communities vorangetrieben. So stellt der Einsatz von Grid-fähigen Applikationen in medizinischen oder vorwiegend kommerziellen Bereichen weitaus höhere Anforderungen an Infrastrukturen zur Authentifizierung und Autorisierung, als sich mit bisher vorhandenen Lösungen realisieren lassen.

[5] http://www.opsec.com/

[6] http://grid.ncsa.uiuc.edu/GridShib/

Die dargestellte Situation und mögliche komplexe Lösungen bezüglich des Einsatzes von Firewalls in Grid-Umgebungen zeigen exemplarisch die bestehenden Probleme in diesem Bereich. Generell lässt sich festhalten, dass derzeit keine geeigneten Mechanismen für die Einbindung von Firewalls in Grid-Umgebungen existieren. Auch der Einsatz von Web Services bietet hier keine Abhilfe, da lediglich die Kontroll- und Steuerungsinformationen zwischen den Grid-Komponenten ausgetauscht werden. Die eigentlichen Datentransfers erfolgen weiterhin über GridFTP. Abschließend sei angemerkt, dass die Tunnelung sämtlicher Informationen über ausgewiesene Ports für Web Services zwar die Durchschaltung durch Firewalls administrativ vereinfacht, keinesfalls jedoch eine Erhöhung der eigentlichen Sicherheit mit sich bringt.

Die insgesamt in diesem Beitrag dargestellten Entwicklungen betreffen nicht primär die Nutzer von Grid-Applikationen, sondern die Entwickler und Betreiber der erforderlichen Netzinfrastrukturen. Daher ist aus Sicht eines Rechenzentrums zumindest mittelfristig die Auseinandersetzung mit diesen neuen Technologien dringend geboten. Dabei sei ausdrücklich darauf hingewiesen, dass die Grid Middleware auch in den kommenden Jahren stetigen Änderungen unterworfen sein wird. So weisen die in diesem Frühjahr veröffentlichen Versionen des Globus Toolkit 4.0 und gLite zahlreiche Verbesserungen hinsichtlich der Sicherheitsanforderungen auf. Jedoch sind verschieden Module noch nicht vollständig oder stabil implementiert und dokumentiert, so dass ein Produktionsbetrieb mit beiden Middlewares derzeit noch nicht möglich ist.

Literatur

[DAH+04] Denis, A., Aumage, O., Hofman, R., Verstoep, K., Kielmann T., Bal, H. E. *Wide-Area Communication for Grids: An Integrated Solution to Connectivity, Performance and Security Problems*. Proc. 13th IEEE Int. Symposium on High-Performance Distributed Computing, Honolulu, 2004.

[DDF+02] Della-Lebera, G., Dixon, B., Farrell, J., Garg, P., et al. *Security in a Web Services World: A Proposed Architecture and Roadmap*. Version 1.0, 7. April 2002. http://www-128.ibm.com/developerworks/library/ws-secmap/

[FBA+03] Ferreira, L., Berstis, V., Armstrong, J,. Kendzierski, M., et al. *Introduction to Grid Computing with Globus*. IBM Redbook SG24-6895-01, September 2003. http://www.redbooks.ibm.com/redbooks/pdfs/sg246895.pdf

[FKT01] Foster I., Kesselman C.,Tuecke S. *The anatomy of the grid: Enabling scalable virtual organizations*. International J. of Supercomputer Applications, 15(3), 2001.

[GGM04] Green, M. L., Gallo, S. M., Miller, R. *Grid-enabled Virtual Organization Based Dynamic Firewall*. Proc. 5th IEEE/ACM Int. Workshop on Grid Computing, Pittsburgh, 2004.

[GMH04] Groep, D., Mulmo, O., Hahkala, J. *Gap analysis presentation*. In 1st JRA3/MWSG Workshop. 14. Mai 2004.

[Hil02] Hillier, J. *The use of firewalls in the U.K. e-Science grid: ETF Level 2 and beyond*. Version 0.1, 24. Oktober 2002. http://e-science.ox.ac.uk/events/firewall-workshop/FirewallIdeas.pdf

[HMN02] Hondo, M., Melgar, D., Nadalin, A., *Web Services Security: Moving up the stack*. 1. Dezember 2002. http://www-106.ibm.com/developerworks/library/ws-secroad/

[MOV96] Menezes, A., Oorschot, P. v., Vanstone, S. *Handbook of Applied Cryptography*. CRC Press, Oktober 1996. http://www.cacr.math.uwaterloo.ca/hac/

[NaRi04] Naqvi, S., Riguidel, M. *Problems in the Implementation of Grid Security Services*. Proc. Cracow Grid Workshop '04, Kraków, 2004.

[Wel03] Welch, V. *Globus Toolkit Firewall Requirements*. Version 6, 19. Mai 2005. http://www.globus.org/toolkit/security/firewalls/Globus%20Firewall%20Requirements-6.pdf

[Wel04] Welch, V., et. al. *Globus Toolkit Version 4 Grid Security Infrastructure: A Standards Perspective*. Version 2, 8. Dezember 2004. http://www.globus.org/toolkit/docs/4.0/security/GT4-GSI-Overview.pdf